PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-014441

(43)Date of publication of application : 19.01.2001

---

(51)Int.Cl. G06K 19/073
G06F 12/14
G06K 17/00
H04L 9/32

---

(21)Application number : 11-374788 (71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 28.12.1999 (72)Inventor : HIROTA TERUTO
TATEBAYASHI MAKOTO
YUGAWA YASUHEI
MINAMI MASANAO
KOZUKA MASAYUKI

---

(30)Priority
Priority number : 11119441
Priority date : 27.04.1999
Priority country : JP

---

(54) SEMICONDUCTOR MEMORY CARD AND READER

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a semiconductor memory card usable as a storage medium for digital literary works and also usable as a storage medium for general computer data (non-literary works) for which the protection of copyright is not required.
SOLUTION: This card is composed of a control IC 302, a flash memory 303 and a ROM 304, the ROM 304 holds a medium ID 341 or the like peculiar to this card, the flash memory 303 has an authentication area 332 for permitting access to external equipment only when the authentication of that external equipment is made successful and a non-authentication area 331 for permitting access regardless of the authenticated result and the control IC 302 has control parts 325 and 326 for controlling access from the external equipment to the authentication area 332 and the non-authentication area 331 and an authentication part 321 or the like for executing mutual authentication with the external equipment.

LEGAL STATUS [Date of request for examination] 19.04.2002
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3389186
[Date of registration] 17.01.2003
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] It is a semi-conductor memory card removable on electronic equipment. Rewritable nonvolatile memory, It has the control circuit which controls access by said electronic equipment to the authentication field and the non-attesting field which are two storage regions where it was beforehand set in said nonvolatile memory. Said control circuit The non-attesting field access-control section which controls access by said electronic equipment to said non-attesting field, The semi-conductor memory card characterized by having the authentication section which tries authentication of said electronic equipment in order to verify the justification of said electronic equipment, and the authentication field access-control section which permits access by said electronic equipment to said authentication field only when said authentication section succeeds in authentication.
[Claim 2] It is the semi-conductor memory card according to claim 1 characterized by for said authentication section generating the key data reflecting the result of authentication, decoding said authentication field access-control section by the key data by which said authentication section generated the enciphered instruction which is sent from said electronic equipment, and controlling access to said authentication field according to the decoded instruction.
[Claim 3] Said authentication section is a semi-conductor memory card according to claim 2 characterized by generating said key data from the response data generated in order to prove the challenge data transmitted to said electronic equipment in order to perform mutual recognition of said electronic equipment and a challenge response

mold and to verify the justification of said electronic equipment, and self justification.
[Claim 4] The enciphered instruction which is sent from said electronic equipment It consists of the tag section which specifies the classification of access to said authentication field and which is not enciphered, and enciphered address part which pinpoints the field to access. Said authentication section The semi-conductor memory card according to claim 3 characterized by carrying out execution control of the access of the classification specified by the tag section of said instruction to the field which decodes the address part of said instruction and is pinpointed by the decoded address using said key data.
[Claim 5] It is the semi-conductor memory card according to claim 4 characterized by equipping said semi-conductor memory card with the discernment data store circuit which memorizes beforehand the discernment data of the proper which can specify self in distinction from the semi-conductor memory card of further others, for said authentication section performing mutual recognition using the discernment data stored in said discernment data store circuit, making it dependent on said discernment data, and generating said key data.
[Claim 6] Said semi-conductor memory card is a semi-conductor memory card according to claim 1 characterized by having further the area-size modification circuit which changes the area size of said authentication field and each of said non-attesting field.
[Claim 7] It is the semi-conductor memory card according to claim 6 which said authentication field and said non-attesting field are assigned to each field obtained by carrying out the storage region where the fixed size in said nonvolatile memory continued for 2 minutes, and is characterized by said area-size modification circuit changing the area size of said authentication field and each of said non-attesting field by changing the boundary address which carries out the storage region of said fixed size for 2 minutes.
[Claim 8] The authentication field translation table showing correspondence with the logical address and a physical address, [in / in said area-size modification circuit / said authentication field] The non-attesting field translation table showing correspondence with the logical address and the physical address in said non-attesting field, It has the translation table modification section which changes said authentication field translation table and said authentication field translation table according to the instruction from said electronic equipment. Said authentication field access-control section It is the semi-conductor memory card according to claim 7 characterized by controlling access by said electronic equipment based on said

authentication field translation table, and said non-attesting field access-control section controlling access by said electronic equipment based on said non-attesting field translation table.

[Claim 9] It is the semi-conductor memory card according to claim 8 to which said authentication field and said non-attesting field are assigned to the high field and the low field of the physical address obtained by carrying out the storage region of said fixed size for 2 minutes, respectively, the logical address and a physical address are matched so that, as for said non-attesting field translation table, the ascending order of the logical address may turn into ascending order of a physical address, and said authentication field translation table is characterized by matching the logical address and a physical address so that the ascending order of the logical address may turn into descending order of a physical address.

[Claim 10] Said semi-conductor memory card is a semi-conductor memory card according to claim 1 characterized by having the read-only memory circuit in which data were stored further beforehand.

[Claim 11] Said authentication field and said non-attesting field consist of a storage region which can be written for said electronic equipment, and a read-only storage region. Said control circuit has the random number generator which generates a random number whenever it accesses further for said electronic equipment writing data in said nonvolatile memory. Said authentication field access-control section and said non-attesting field access-control section The semi-conductor memory card according to claim 1 characterized by writing said random number in said read-only storage region matched with said encryption data while enciphering and writing said data in the storage region which can write [said] the obtained encryption data using said random number.

[Claim 12] Said control circuit is a semi-conductor memory card according to claim 1 which has further the translation table showing correspondence with the logical address and the physical address in said authentication field and said non-attesting field, and the translation table modification section which changes said translation table according to the instruction from said electronic equipment, and is characterized by said authentication field access-control section and said non-attesting field access-control section controlling access by said electronic equipment based on said translation table.

[Claim 13] Said control circuit is a semi-conductor memory card according to claim 1 characterized by having the code decode section which decrypts the data read from said authentication field and said non-attesting field while enciphering further the data

which should be written in said authentication field and said non-attesting field.
[Claim 14] It is the semi-conductor memory card according to claim 1 characterized by for said nonvolatile memory being a flash memory and having the non-eliminated list read-out section which sends the information which said control circuit pinpoints the field which is not eliminated [which exists in said authentication field and said authentication field further according to the instruction from said electronic equipment], and shows the field to said electronic equipment.
[Claim 15] The user key storage section for said authentication section to require the user key which is the information on a proper of the user from the user who uses electronic equipment for authentication, and for said control circuit memorize said user key further, The identification information storage section for memorizing the identification information which can specify the electronic equipment which succeeded in authentication by said authentication section, If authentication by said authentication section is started, identification information will be acquired from the electronic equipment. The semi-conductor memory card according to claim 1 characterized by having the user key demand prohibition section in which the demand of the user key by said authentication section is forbidden when the identification information inspects whether it is already stored in said identification information storage section and is already stored in it.
[Claim 16] It is read-out equipment which reads the digital work stored in the semi-conductor memory card according to claim 1. Said semi-conductor memory card While the digital work is stored in the non-attesting field, the count which permits read-out of said digital work is beforehand stored in an authentication field. Said read-out equipment A decision means to judge whether the count stored in said authentication field is read, and read-out is permitted by the count in case the digital work stored in said non-attesting field is read, Read-out equipment characterized by having the playback means which subtracts said read count and is returned to said authentication field while reading said digital work from said non-attesting field, only when the permission is granted.
[Claim 17] It is read-out equipment which reads the digital work stored in the semi-conductor memory card according to claim 1, and is reproduced to an analog signal. Said semi-conductor memory card While the digital work refreshable to an analog signal is stored in the non-attesting field A playback means to read the digital work with which the count which permits the digital output by said electronic equipment of said digital work was beforehand stored in the authentication field, and was stored in it to said read-out equipment and said non-attesting field, and to

reproduce to an analog signal, Only when the permission is granted with a decision means to judge whether the count stored in said authentication field is read, and the digital output is permitted by the count, while outputting said digital work outside with a digital signal Read-out equipment characterized by having the digital output means which subtracts said read count and is returned to said authentication field.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the suitable semi-conductor memory card for protection of copyrights and read-out equipment of a digital work especially about the semi-conductor memory card and its read-out equipment for memorizing a digital work etc.

[0002]

[Description of the Prior Art] Digital works, such as a music content, come to be distributed by development of a multimedia network technique through communication networks, such as the Internet, in recent years, and it has become possible to touch the music in the world etc. at a house. For example, after downloading a music content with a personal computer (henceforth "PC"), music can be played and enjoyed by storing in the semi-conductor memory card with which PC was equipped if needed. Moreover, music can also be listened to with a walk by taking out from PC the

semi-conductor memory card which did in this way and stored the music content, and equipping a pocket mold music regenerative apparatus. Such semi-conductor memory cards are non-volatiles, such as a flash memory, and are convenient small lightweight cards which contained the semiconductor memory of big storage capacity.

[0003] By the way, when memorizing a digital work to a semi-conductor memory card, in order to prevent an unjust copy, in such an electronic music distribution, it is necessary to use a key etc. and to encipher contents. Moreover, it is necessary to prevent from copying to other storages etc. depending on the file management software which standard attachment was carried out at PC etc. and has appeared on the market widely.

[0004] The policy which enables access to a semi-conductor memory card only by the software of dedication as an approach of preventing such an unjust copy can be considered. For example, when authentication between PC and a semi-conductor memory card is successful and it cannot succeed in the authentication since it supposes that access to a semi-conductor memory card is permitted and there is no software of dedication, the approach of supposing that access to a semi-conductor memory card is forbidden can be considered.

[0005]

[Problem(s) to be Solved by the Invention] However, in the software of dedication always being needed for PC accessing a semi-conductor memory card, it will become impossible to carry out the data exchange mutually freely through the unspecified user and unspecified semi-conductor memory card which do not own the software of such dedication. Therefore, the convenience that PC can be accessed by the file management software by which standard attachment is carried out is no longer acquired, without needing the convenience which the conventional semi-conductor memory cards, such as a flash plate ATA and CompactFlash, had, i.e., the software of dedication.

[0006] That is, although it is suitable as a storage of a digital work in that an accessible semi-conductor memory card has the function of protection of copyrights only by the software of dedication, since general-purpose use is difficult, there is a trouble that it cannot be used as an auxiliary storage unit in a general computer system. Then, this invention is made in view of such a trouble, and aims at offering the semi-conductor memory card [using as a storage of a digital work is possible and] which can be used also as a storage of the common computer data (non-work) for which protection of copyrights is not needed, and its read-out equipment.

[0007]

[Means for Solving the Problem] In order to attain the above-mentioned purpose, the semi-conductor memory card concerning this invention It is a semi-conductor memory card removable on electronic equipment. Rewritable nonvolatile memory, It has the control circuit which controls access by said electronic equipment to the authentication field and the non-attesting field which are two storage regions where it was beforehand set in said nonvolatile memory. Said control circuit The non-attesting field access-control section which controls access by said electronic equipment to said non-attesting field, It is characterized by having the authentication section which tries authentication of said electronic equipment in order to verify the justification of said electronic equipment, and the authentication field access-control section which permits access by said electronic equipment to said authentication field only when said authentication section succeeds in authentication.

[0008] Here, said semi-conductor memory card may be further equipped with the area-size modification circuit which changes the area size of said authentication field and each of said non-attesting field. The read-out equipment concerning this invention is read-out equipment which reads the digital work stored in the above-mentioned semi-conductor memory card. Moreover, said semi-conductor memory card While the digital work is stored in the non-attesting field, the count which permits read-out of said digital work is beforehand stored in an authentication field. Said read-out equipment A decision means to judge whether the count stored in said authentication field is read, and read-out is permitted by the count in case the digital work stored in said non-attesting field is read, Only when the permission is granted, while reading said digital work from said non-attesting field, it is characterized by having the playback means which subtracts said read count and is returned to said authentication field.

[0009]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained using a drawing. Drawing 1 is PC which downloads digital works, such as a music content, through a communication network, and drawing showing the appearance of a removable semi-conductor memory card (only henceforth a "memory card") in the PC.

[0010] PC102 is equipped with a display 103, a keyboard 104, and loudspeaker 106 grade, and is connected to the communication line 101 by the modem to build in. And the memory card writer 107 is inserted in card slots (memory card writer insertion opening 105), such as PCMCIA which this PC102 has. The memory card writer 107 is an adapter which connects PC102 and a memory card 109 electrically, and the

memory card insertion opening 108 is equipped with the memory card 109.

[0011] By using such a system, a user can acquire the music data which the content provider on the Internet offers by passing through the following procedures. First, a user downloads a desired music content to the hard disk of the PC102 interior through a communication line 101. It is enciphered, and if music data remain as it is, they are unreproducible in PC102.

[0012] In order to reproduce, it is necessary to pay money using a credit card etc. to the content provider of a downloading agency. If payment is finished, a password and right information can come to hand from a content provider. A password is key data required to cancel the enciphered music data. Right information is information which shows the playback conditions permitted to users who show the count of refreshable in PC, the count to a memory card which can be written in, and a refreshable period, such as a playback term.

[0013] The user who acquired a password and right information enters the password which came to hand from a keyboard 104 to the application program (this program is only hereafter called "application".) of dedication to which the copyright protection feature was attached, when carrying out the playback output of the music from the loudspeaker 106 of PC102. Then, the application carries out a playback output as voice through a loudspeaker 106, decoding the enciphered music data using a password, after checking right information.

[0014] Moreover, when the writing to a memory card is permitted as right information, the application can write the enciphered music data, a password, and right information in a memory card 109. Drawing 2 is drawing showing the appearance of the recorded message sender for telephone (henceforth a "player") 201 of the pocket mold which uses this memory card 109 as a record medium.

[0015] The liquid crystal display section 203 and a manual operation button 202 are formed in the top face of a player 201, the communication link ports 213, such as USB for connecting with the memory card insertion opening 206 for detaching and attaching a memory card 109 and PC102 grade, are established in a near-side side, and the analog output terminal 204, the digital output terminal 205, and the analog input terminal 223 grade are prepared in the right lateral.

[0016] If it is in the condition that playback is permitted, based on the music data stored in the memory card 109, a password, and right information, after a player 201 reads and decodes the music data, it is changed into an analog signal, and through the headphone 208 connected to the analog output terminal 204, it will output as voice or it will output the music data under playback to the digital output terminal 205 with

digital data.

[0017] Moreover, this player 201 can record the music data, the password, and right information which were downloaded with that PC102 on a memory card 109 by changing into digital data the sound signal of an analog inputted from the analog input terminal 223 through a microphone etc., recording on a memory card 109 or communicating with PC102 connected through the communication link port 213. That is, this player 201 has the function to replace PC102 shown in drawing 1 , and the memory card writer 107, about playback of the music data recorded on record and the memory card 109 of the music data to a memory card 109.

[0018] Drawing 3 is the block diagram showing the hardware configuration of PC102. PC102 USB for connecting with the modem port for connecting with ROM111, RAM112, the display 103, and communication line 101 which have memorized beforehand CPU110, device key 111a, control program 111b, etc., or a player 201 etc. The memory card writer 107 which connects the communication link port 113 which it has, a keyboard 104, an internal bus 114, and a memory card 109 and an internal bus 214, the descrambler 1117 which decodes the encryption music data read from the memory card 109, and the decoded music data The AAC decoder 118 based on MPEG 2-AAC (ISO 13818-7) to elongate, D/A converter 119 which changes the elongated digital music data into an analog sound signal, a loudspeaker 106 and file management software, and application It consists of stored hard disk 120 grades.

[0019] This PC102 is performing file management software stored in the hard disk 120. It not only can use as an auxiliary storage unit which has the file system (ISO9293 grade) which became independent like a hard disk about the memory card 109, but By performing above-mentioned exclusive application stored in the hard disk 120 The modem of the communication link port 113 etc. is minded. Download a music content etc. from a communication line 101, or After performing mutual recognition with a memory card 109, a music content etc. is stored in a memory card 109, or the music content stored in the memory card 109 is read, and a playback output is carried out at a loudspeaker 106.

[0020] In addition, device key 111a stored in ROM111 is used for mutual recognition etc. so that it may be the private key of a proper and may mention later to this PC102. Drawing 4 is the block diagram showing the hardware configuration of a player 201. A player 201 The communication link ports 213, such as USB for connecting with ROM211, RAM212, the liquid crystal display section 203, and PC102 grade which have memorized beforehand CPU210, device key 211a, control program 211b, etc., a manual operation button 202, an internal bus 214, A memory card 109 and an internal bus 214

The card I/F section 215 to connect, the authentication circuit 216 which performs mutual recognition with a memory card 109, the descrambler 217 which decodes the encryption music data read from the memory card 109, decoded MPEG 2-AAC which carries out music data elongation The analog music signal inputted from the AAC decoder 218 based on (ISO 13818-7), D/A converter 219 which changes the elongated digital music data into an analog sound signal, the loudspeaker 224, and the analog input terminal 223 A/D converter 221 which changes into digital music data, and its digital music data are based on MPEG 2-AAC (ISO 13818-7). It consists of the AAC encoder 220 which carries out compression coding, the scrambler 222 which enciphers the music data by which compression coding was carried out, an analog output terminal 204, a digital output terminal 205, and an analog input terminal 223.

[0021] It is loading control program 211b stored in ROM211 to RAM212, and performing CPU210, and this player 201 reads the music content stored in the memory card 109, and a playback output is carried out or it stores in a loudspeaker 224 the music content inputted through the analog input terminal 223 or the communication link port 213 at a memory card 109. That is, it can record music individually, or it can reproduce and it not only can enjoy itself, but it can perform record and playback of the music content concerning the electronic music distribution downloaded with PC102 (protection of copyrights is needed) like the usual player.

[0022] Drawing 5 is drawing showing the appearance and hardware configuration of a memory card 109. The memory card 109 is carrying out the internal organs of the rewritable nonvolatile memory which can write in repeatedly, and the storage capacity is 64MB and it operates in response to the power source of 3.3V, and supply of a clock signal from the exterior. Moreover, memory cards 109 are 2.1mm in thickness, 32mm long, and a 24mm wide rectangular parallelepiped configuration, they are written in the side face, have a prevention switch (write protect SW), and are electrically connected with an external instrument by the connection terminal of nine pins.

[0023] This memory card 109 builds in three IC chips (control IC 302, a flash memory 303, ROM304). It has the non-attesting field 331 grade which are the authentication field 332 which is a storage region which permits access only to the device which was able to be attested with a flash memory 303 being the nonvolatile memory which can rewrite a package elimination mold, and being a just device as a logical storage region, and the storage region which permits access, without needing such authentication. Here, since the authentication field 332 stores the important data in connection with protection of copyrights, it is used, and the non-attesting field 331 is used as an auxiliary storage unit in a general computer system. In addition, these two storage

regions are classified bordering on the fixed address on a flash memory 303.

[0024] ROM304 has the read-only storage region called a special field, and has held beforehand the information on the manufacture manufacture name 342 grade of the media ID 341 which are the identification information of a proper, and this memory card 109 to this memory card 109. In addition, it is discernment data of the proper which can specify self in distinction from other semi-conductor memory cards, and media ID 341 are used for the mutual recognition between devices, and they are used here in order to prevent unjust access to the authentication field 332.

[0025] Control IC 302 is a control circuit which consists of active components (logic gate etc.), and has the authentication section 321, the command judging control section 322, the master key storage section 323, the special field access-control section 324, the authentication field access-control section 325, the non-attesting field access-control section 326, and a code and decryption circuit 327 grade. The authentication section 321 is a circuit which performs mutual recognition of the phase hand-loom machine which is going to access this memory card 109, and a challenge response mold, and attests the justification of a phase hand-loom machine by detecting whether it has a random number generator, a code machine, etc., and the phase hand-loom machine has the same code machine as that code machine. With in addition, the mutual recognition of a challenge response mold Challenge data in a phase hand-loom vessel in order to verify the justification of a phase hand-loom machine Delivery, The response data with which **** generation of the processing which proves self justification in a phase hand-loom machine to it was carried out in **** From a phase hand-loom machine to reception It is that both devices perform mutually the authentication step of judging whether a phase hand-loom machine being attested by comparing these challenge data with response data.

[0026] The command judging control section 322 is a controller which consists of a decoding circuit which judges and performs the class of command (instruction to this memory card 109) inputted through the command pin, or a control circuit, and controls the various components 321-327 according to the class of inputted command. a command -- the data of a flash memory 303 -- reading - writing - not only the command to eliminate but the commands (an address space, command about non-eliminated data, etc.) for controlling a flash memory 303 are contained.

[0027] For example, about R/W of data, the command "SecureRead address count" for accessing the authentication field 332, "SecureWrite address count", the command "Read address count" for accessing the non-attesting field 331, "Write address count", etc. are defined. Here, "address" is the number of the sector of the

beginning of a series of sector groups set as the object of R/W, and "count" shows the number of sum total sectors to write. Moreover, a sector is a unit at the time of writing data to a memory card 109, and is 512 bytes here.

[0028] The master key storage section 323 has memorized beforehand master key 323a used in order for a phase hand-loom machine to use in the case of mutual recognition or to protect the data in a flash memory 303. The special field access-control section 324 is a circuit which reads the media ID341 grade stored in the special field (ROM304).

[0029] The authentication field access-control section 325 and the non-attesting field access-control section 326 are circuits which perform data writing and read-out to the authentication field 332 and the non-attesting field 331 of a flash memory 303, and data are transmitted, respectively and received between external instruments (PC102 and player 201 grade) through four data pins. In addition, when rewriting the contents of the flash memory 303, a block (32 sectors, 16 K bytes) is outputted [these access-controls sections 325 and 326 / although it has the buffer memory for 1 block inside and a sector is logically outputted and inputted as a unit (access on a command with an external instrument)] and inputted as a unit. When rewriting one certain sector data, while reading the block which corresponds from a flash memory 303 to buffer memory and specifically carrying out package elimination of the block, after rewriting the applicable sector in buffer memory, the block is returned to a flash memory 303 from buffer memory.

[0030] It is the circuit which performs encryption and a decryption using master key 323a stored in the master key storage section 323 under control by the authentication field access-control section 325 and the non-attesting field access-control section 326, in case a code and the decryption circuit 327 write data in a flash memory 303, it enciphers and writes in the data, and when it reads data from a flash memory 303, it decrypts the data. This is for preventing a malfeasance, such as stealing the password which the inaccurate user decomposed this memory card 109, analyzed the contents of the flash memory 303 directly, and was stored in the authentication field 332.

[0031] In addition, control IC 302 has the synchronous circuit which generates the internal clock signal which synchronized with the clock signal supplied from a clock pin besides these main components 321-327, and is supplied to each component, an volatile storage region, the storage region of a non-volatile, etc. Moreover, in order to prevent the alteration of the information stored in the special field (ROM304), the ROM304 may be made to build in in control IC 302, or those information may be stored in a flash memory 303, and the special field access-control section 324 may apply a

limit so that it cannot write in from the outside. It is good also as then storing the data enciphered in the code and the decryption circuit 327.

[0032] Drawing 6 is drawing showing the class of storage region of the memory card 109 seen from PC102 or the player 201. The storage region which a memory card 109 has is roughly divided, and are three fields, the special field 304, the authentication field 332, and the non-attesting field 331. The special field 304 is a read-only field, and reads to the data in this using a device dependent command. The authentication field 332 is a field whose R/W is possible, only when authentication is successful between PC102 or a player 201, and a memory card 109, and the enciphered command is used for it about access to this field. The non-attesting field 331 is a field which can be written without accessing namely, attesting by the command exhibited [SCSI / ATA,]. Therefore, to the non-attesting field 331, R/W of data is possible by the file management software on PC102 like a flash plate ATA and CompactFlash.

[0033] It supposes that the following information is stored and three storage regions are provided with the function and the function of protection of copyrights to the music data concerning an electronic music distribution as an auxiliary storage unit of common PC by this. That is, the user data 427 grade which is common data with unrelated encryption contents 426 as which the music data set as the object of protection of copyrights were enciphered and protection of copyrights is stored in the non-attesting field 331. The cryptographic key 425 used as the private key for decoding the encryption contents 426 stored in the non-attesting field 331 is stored in the authentication field 332. And the media ID 341 which are the information needed in order to access the authentication field 332 are stored in the special field 304.

[0034] PC102 and a player 201 read the media ID 341 first stored in the special field 304 of the memory card 109 with which it was equipped, and take out the cryptographic key 425 and right information which were stored in the authentication field 332 using it. If playback is permitted using these cryptographic keys 425 or right information, it is reproducible, reading the encryption contents 426 in the non-attesting field 331, and decoding by the cryptographic key 425.

[0035] A certain user writes only the music data which came to hand unjustly in the non-attesting field 331 of a memory card 109 in PC102 grade, and presupposes that the player 201 tended to be equipped with such a memory card 109, and it was going to reproduce. However, although music data are stored in the non-attesting field 331 of the memory card 109, since the cryptographic key 425 or right information corresponding to the authentication field 332 do not exist, the player 201 cannot reproduce the music data. Since the music content is not reproduced even if it

reproduces only a music content to a memory card 109 by this without being accompanied by the cryptographic key and right information on normal, the unjust duplicate of a digital work is prevented.

[0036] (a) shows the Ruhr in access to each field, drawing 7 is drawing showing the limit at the time of PC102 and a player 201 accessing each field of a memory card 109, and the gestalt of a command, and (c) is [(b) shows the Ruhr in modification of the size of each field, and] the conceptual diagram showing the field of a memory card 109. The special field 304 is a read-only field, and can be accessed by the device dependent command, without attesting. The media ID 341 stored in this special field 304 are used for the generation and the decode of an encryption command for accessing the authentication field 332. That is, PC102 and a player 201 read these media ID 341, encipher the command which accesses the authentication field 332 using this, and send it to a memory card 109. On the other hand, the memory card 109 which received the encryption command decodes, interprets and executes the encryption command using media ID 341.

[0037] The authentication field 332 is a field whose access is attained, only when authentication is successful between the equipment and the memory cards 109 which access the memory card 109 of PC102 or player 201 grade, and the magnitude is equivalent to the sector of an individual (YYYY+1). that is, logically, this authentication field 332 consists of sectors of the 0th - YYYY -- having -- physical -- the [of a flash memory 303] -- it consists of sectors which have the sector address of XXXX - ** (XXXX+YYYY). In addition, sector addresses are a series of numbers uniquely attached to each of all sectors that constitute a flash memory 303.

[0038] The non-attesting field 331 can be accessed by standard commands, such as ATA and SCSI, without attesting, and the magnitude is equivalent to the sector of XXXX individual. That is, also logically and physically, this non-attesting field 331 consists of the 0th - (XXXX-1) a sector. In addition, the alternative block field 501 which consists of an assembly of the shift block for substituting for the defective block (block which has the storage region of the defect who cannot write normally) produced to the authentication field 332 or the non-attesting field 331 may be beforehand assigned to a flash memory 303.

[0039] Moreover, although the special field 304 can be accessed without authentication, in order to prevent the analysis from an inaccurate user, though it cannot access unless it comes out, after attesting, it is good, and the command which accesses the special field 304 may be enciphered. next, drawing 7 (b) and (c) -- using -- the authentication field 332 and the non-attesting field 331 -- how to change each

area size is explained.

[0040] Although the memory capacity of the sum total of the authentication field 332 and the non-attesting field 331 which are established in a flash memory 303 is the fixed value except all the storage regions of a flash memory 303 to alternative block field 501 grade, a part for i.e., the sector of an individual (XXXX+YYYY +1), each magnitude is changing the value of the boundary address XXXX, and serves as adjustable.

[0041] In order to change area size, it attests first. This is because magnitude cannot be easily changed using the software which performs standard program wide opened widely by the user of PC, and unjust access. After attesting, it is the device dependent command of field modification, and the magnitude (the new number XXXX of sectors) of the non-attesting field 331 is sent to a memory card 109.

[0042] If the field change command is received, a memory card 109 will save the value XXXX in a working area [**** / in a memory card 109 / un-] etc., and will perform the access control to the authentication field 332 and the non-attesting field 331 by making the value into the new boundary address in subsequent accesses. that is, -- while assigning the physical sector of the 0th - XXXX on a flash memory 303 to the non-attesting field 331 -- the -- the sector of eye watch [XXXX - (XXXX+YYYY)] is assigned to the authentication field 332. And based on such new memory mapping, the access-control sections 325 and 326 change the logical address and a physical address, or supervise generating of violation of access exceeding a field. In addition, the logical address is the address in the data space (on a command) at the time of seeing a memory card 109 from an external instrument, and a physical address is the address in the data space which has the flash memory 303 of a memory card 109.

[0043] Here, when size of the authentication field 332 is enlarged by making the boundary address small, in order to maintain logical compatibility with modification before, the allowance of moving all the data stored in the authentication field 332 is needed. For that purpose, what is necessary is only for the movement magnitude of the boundary address to move all data in the direction of low order of the address (copy), and just to change correspondence relation, for example so that a new physical address may be equivalent to the logical address which begins from the new boundary address. The data space is expanded maintaining the logical address of the data stored in the authentication field 332 by this.

[0044] In addition, it is good also as enciphering and using a command also about the device dependent command for field modification from a viewpoint which prevents unjust access. Drawing 8 is the flow Fig. showing the actuation in which PC102 (and

player 201) writes contents, such as music data, in a memory card 109. Here, the case (S601) where PC102 writes in a memory card 109 is explained.

[0045] (1) If PC102 performs authentication of the authentication section 321 of a memory card 109, and a challenge response mold and succeeds in the authentication using device key 111a etc., it will take out master key 323a from a memory card 109 first (S602).

(2) Next, take out the media ID 341 stored in the special field 304 of a memory card 109 using a device dependent command (S603).

[0046] (3) Then, generate a random number and generate the password for enciphering music data from the random number, and master key 323a and Media ID 341 which were taken out now (S604). For example, in the above-mentioned authentication, what enciphered the challenge data (random number) transmitted to the memory card 109 is used for the random number at this time.

(4) Encipher the obtained password by master key 323a and media ID 341, and write in the authentication field 332 as a cryptographic key 425 (S605). At this time, before transmitting data (cryptographic key 425), the command for writing in the authentication field 332 is enciphered, and it transmits to the memory card 109.

[0047] (5) Finally store in the non-attesting field 331 as encryption contents 426, enciphering music data with a password (S606). Drawing 9 is the flow Fig. showing the actuation which reads contents, such as music data, from a memory card 109, and is reproduced by the player 201 (and PC102). Here, the case (S701) where a player 201 reproduces the music data in a memory card 109 is explained.

[0048] (1) If a player 201 performs authentication of the authentication section 321 of a memory card 109, and a challenge response mold and succeeds in the authentication using device key 211a etc., it will take out master key 323a from a memory card 109 first (S702).

(2) Next, take out the media ID 341 stored in the special field 304 of a memory card 109 using a device dependent command (S703).

[0049] (3) Then, take out the music data encryption key 425 from the authentication field 332 of a memory card 109 (S704). At this time, the command for reading from the authentication field 332 is enciphered in advance of read-out of data (cryptographic key 425), and it transmits to the memory card 109.

(4) Decrypt the obtained cryptographic key 425 by master key 323a and media ID 341, and extract a password (S705). The decryption at this time is the inverse transformation of encryption at step S605 shown in drawing 8 .

[0050] (5) Finally, read the encryption contents 426 from the non-attesting field 331,

and play music, decoding with the password extracted at the above-mentioned step S705 (S706). Thus, the music data stored in the non-attesting field 331 of a memory card 109 cannot be decoded if there is no cryptographic key 425 of the authentication field 332. Therefore, since the music data is normally unreproducible even if it copies only music data to injustice at another memory card, the copyright of the music data is protected by insurance.

[0051] Moreover, since access to the authentication field of a memory card is permitted, the protection of copyrights of permitting access to the authentication field of a memory card only to the device which filled certain conditions with choosing appropriately a device key, encryption algorithm, etc. which are used for authentication, and using them only of the device which succeeded in authentication becomes possible. In addition, although the password used for that encryption was enciphered by the master key and Media ID and it was stored in the authentication field 332 as a cryptographic key in this example when recording encryption contents on a memory card 109 (S605), it is good also as enciphering using either a master key and the media ID. The advantage that the circuit scale of a memory card 109 or player 201 grade becomes small with simplification of encryption by this although there is a possibility that the reinforcement of a code may fall is acquired.

[0052] Moreover, according to authentication, although the player 201 and PC102 took out master key 323a from the memory card 109, they may embed the master key 323a beforehand at a player 201 or PC102, may encipher master key 323a, and may store it in the special field 304 as an encryption master key. Next, the example which stored "the count of read-out", and the example which stored "the count of digital output authorization" are shown as an example of an activity of the authentication field of such a memory card.

[0053] Drawing 10 is the flow Fig. showing the actuation in which the player 201 (and PC102) was stored in the authentication field of a memory card 109, and which reads and operates a count 812. Here, the case (S801) where reproducing the music data which were stored in the memory card 109 and with which the player 201 was stored in the non-attesting field 331 of a memory card 109 to a sound signal is permitted is explained only within the limits of a count 812 by reading.

[0054] (1) If a player 201 performs authentication of the authentication section 321 of a memory card 109, and a challenge response mold and succeeds in the authentication using device key 211a etc., it will take out master key 323a from a memory card 109 first (S802).

(2) Next, take out the media ID 341 stored in the special field 304 of a memory card

109 using a device dependent command (S803).

[0055] (3) Then, take out the music data encryption key 425 from the authentication field 332 of a memory card 109 (S704). At this time, the command for reading from the authentication field 332 is enciphered in advance of read-out of data (cryptographic key 425), and it transmits to the memory card 109.

(4) Next, read from the authentication field 332 of a memory card 109, take out a count 812, and inspect the value (S804). Consequently, when it is the value of the purport to which read-out with the unrestricted value is permitted, music is played according to the procedure (S704-S706) shown in drawing 9 , and the same procedure (S806-S808).

[0056] (5) On the other hand, when the count 812 of read-out shows 0, judge with playback not being permitted any longer (S805), and end regeneration (S809). When that is not right, the one count 812 of read-out is subtracted, and after returning the result to the authentication field 332, music is played according to (S805) and the above-mentioned procedure (S806-S808).

[0057] Thus, it becomes possible to control the count of the music playback by the player 201 by [which specified the count of playback permitted beforehand as the authentication field 332 of a memory card 109] reading and storing the count 812. It becomes possible to apply to the analog playback by for example, the rental CD, a KIOSK terminal, etc. by this.

[0058] In addition, it can replace with the count 812 of read-out, and the total time amount which can reproduce a music content can also be restricted by considering as "read-out time amount." Moreover, a count and time amount may be combined. Furthermore, the count 812 of read-out may subtract the count, only when continuing being reproduced exceeding fixed time amount, such as 10 etc. seconds, after starting playback. Moreover, the count 812 of read-out is good also as enciphering and storing, in order to prevent an unjust alteration.

[0059] Drawing 11 is the flow Fig. showing the actuation which operates the count 913 of digital output authorization by which the player 201 (and PC102) was stored in the authentication field of a memory card 109. Here, the case (S901) where it is permitted that a player 201 reads and carries out the digital output of the music data stored in the non-attesting field 331 of a memory card 109 only within the limits of the count 913 of digital output authorization stored in the memory card 109 is explained.

[0060] (1) A player 201 extracts the password which takes out master key 323a like the case (S701-S705) of the playback shown in drawing 9 after attesting with a memory card 109 (S902), takes out media ID 341 (S903), and takes out a

cryptographic key 425 (S904) (S905).
(2) Next, take out the count 913 of digital output authorization from the authentication field 332 of a memory card 109, and inspect the value (S906). Consequently, when it is the value of the purport to which a digital output with the unrestricted value is permitted, the encryption contents 426 are read from the non-attesting field 331, and it outputs from the digital output terminal 205 as digital music data, decoding with the password extracted at the above-mentioned step S905 (S909).
[0061] (3) On the other hand, when the count 913 of digital output authorization shows 0, judge with the digital output not being permitted any longer (S908), and perform only playback by analog output (S908). That is, the encryption contents 426 are read from the non-attesting field 331, and music is played, decoding with a password (S908).
(4) When the fixed count of a limit whose count 913 of digital output authorization which it began to read is not 0 is shown, read the encryption contents 426 from (S907) and the non-attesting field 331 after subtracting the one count and returning the result to the authentication field 332, and output from the digital output terminal 205 as digital music data, decoding with the password extracted at the above-mentioned step S905 (S909).
[0062] Thus, it becomes possible to control the count of the digital output of the music data based on a player 201 by storing the count 913 of digital output authorization which specified the count of the digital output permitted beforehand as the authentication field 332 of a memory card 109. By this, the application to the digital playback by for example, the rental CD, a KIOSK terminal, etc., i.e., employment which permits a copy by the count which specified digital dubbing of the music data memorized to the memory card as the origin of comprehension of a copyright person, is realized.
[0063] In addition, like the case of "the count of read-out", it can replace with the count 913 of digital output authorization, and the total time amount which can output a music content with digital data can also be restricted by considering as "digital output authorization time amount." Moreover, a count and time amount may be combined. Furthermore, after the count 913 of digital output authorization starts the output, only when continuing being outputted exceeding fixed time amount, such as 10 etc. seconds, it may subtract the count. Moreover, the count 913 of digital output authorization is good also as enciphering and storing, in order to prevent an unjust alteration.
[0064] Furthermore, the function in which only the count specified by a copyright

person increases the count of digital output authorization by paying price into a copyright person may be added. Next, the physical DS (a sector and structure of an ECC block) of this memory card 109 is explained. In this memory card 109, suitable DS to prevent the malfeasance accompanying backup and restoration of the data stored in the flash memory 303, the malfeasance accompanying the alteration of data, etc. is adopted. That is, above "counts of read-out" and "the counts of digital output authorization" may be stored in the authentication field 332, and the following attacks may be received by the method counted down whenever it performs these actions.

[0065] That is, when music playback is repeated and these counts are set to 0 after backing up the stored data of the flash memory 303 whole to an external auxiliary storage unit etc., by restoring backup data, music playback can be repeated again or it is possible [it] to repeat music playback unjustly altering the "count of read-out" itself. Therefore, the allowance which prevents such an action is needed.

[0066] Drawing 12 is drawing showing DS common to the authentication field 332 and the non-attesting field 331 of a memory card 109, and the flow of the R/W processing corresponding to the DS. the counter value which the random number generator 1003 which the authentication section 321 grade of control IC 302 has generates here -- the time -- as a strange key -- using -- having .

[0067] 16 bytes of extended partition 1005 is assigned to a flash memory 303 512 bytes of every sector 1004. The data with which each sector was enciphered with the counter value are stored. An extended partition 1005 consists of a strange field 1007 at the time of 8 bytes for storing the counter value used for generation of the 8 bytes of ECC data 1006 and encryption data for storing the error correcting code of the encryption data stored in the corresponding sector.

[0068] In addition, logically (using the command wide opened by the user), an accessible field is only a sector 1004 and an extended partition 1005 is a field where it is accessible that it is only physical (as control by the equipment which write a memory card). even if only sector data are altered by considering as such DS using a command etc. -- the time -- strange -- since the contents of field 1007 are not changed, an unjust alteration can be prevented by using those adjustments.

[0069] Specifically, PC102 and a player 201 store or read data to the authentication field 332 and the non-attesting field 331 of a flash memory 303 according to the following procedures every sector 1004. Here, a procedure in case PC102 writes data in a memory card 109 (S1001) is explained first.

(1) PC102 requires issue of a counter value from a memory card 109. Then, the control IC 302 in a memory card 109 generates a random number with the internal

random number generator 1003 (S1005), and sends it to PC102 grade by making the random number into a TAUNTA value (S1002).

[0070] (2) Generate a password from the acquired counter value, and master key 323a and Media ID 341 which are already acquired (S1003).

(3) Send to a memory card 109, enciphering with a password the data for 1 sector which should be written in (S1004). At this time, the (4) memory card 109 which also sends the information which specifies the sector which should be written in, and the counter value used for encryption together writes the received encryption data in the specified sector 1004 (S1006).

[0071] (5) Calculate ECC from the encryption data and write in the extended partition 1005 corresponding to the above-mentioned sector as ECC data 1006 (S1007).

(6) then, the counter value received with the above-mentioned encryption data -- the time -- strange -- write in field 1007 (S1008). Next, a procedure in case PC102 reads data from a memory card 109 (S1011) is explained.

[0072] (1) PC102 specifies a sector to a memory card 109 -- require both read-out of data. Then, a memory card 109 reads only the encryption data of the specified sector 1004 first, and outputs them to PC102 (S1016), and PC102 receives the encryption data (S1012).

(2) Next, a memory card 109 reads the counter value stored in the strange field 1007 at the time of the extended partition 1005 corresponding to the specified sector 1004, and outputs it to PC102 (S1017), and PC102 receives the counter value (S1013).

[0073] (3) Generate a password from the counter value which it began to read, and master key 323a and Media ID 341 which are already acquired (S1014).

(4) Decode encryption data using the password (S1015). the case where the data of a sector 1004 are changed by the unjust alteration etc. here -- the time -- strange -- mismatching with the counter value read from field 1007 arises, and it is not restored to the original data.

[0074] Thus, from a user, the strange field 1007 can be formed in a flash memory 303 at the time as a hiding (it cannot access) field which is not visible, and the alteration of the data by the inaccurate user can be prevented by enciphering and storing data with the password depending on the counter value stored there. in addition -- here -- the time -- strange -- although field 1007 considered as the extended partition 1005 for storing ECC, as long as it is a field whose rewriting is impossible from the exterior of a memory card, it may be prepared in other fields in a flash memory 303.

[0075] Moreover, although the counter value was a random number, it is good also as a value which considers as timer values, such as time of day which changes every

moment, or shows the count of writing to a flash memory 303. Next, a desirable example is explained about matching with the logical address of a flash memory 303, and a physical address. Drawing 13 is drawing showing signs that correspondence with the logical address and a physical address is changed, and the translation table 1101 corresponding to [(a)] (a) in (c) and (d) show the translation table 1101 corresponding to (b) corresponding to the correspondence relation after modification in the correspondence relation before modification, and (b).

[0076] Here, it is the table which makes a group all the logical addresses (here number of a logical block), and the physical address (number of the physical block which constitutes a flash memory 303 here) corresponding to each logical address, and memorizes them, a translation table 1101 is saved in a storage region [**** / in control IC 302 / un-] etc., and in case the logical address is changed into a physical address by the authentication field access-control section 325 or the non-attesting field access-control section 326, it is referred to.

[0077] The device which accesses a memory card 109 can write data in not all the data space (all physical blocks that constitute a flash memory 303) that exists physically in a memory card 109, but can write data only in the logical data space (logical block) which can be pinpointed with the logical address. One of the reason of this is because the alternative field for replacing that field must be secured when it becomes impossible to write by damaging a part of flash memory 303. And since the logical continuity of a file it is discontinuous by reflecting modification of the matching in a translation table from the physical block which plurality follows is maintained even if it is the case where such a defective block is replaced with the block in an alternative field, it can be pretended that breakage did not arise to the external instrument.

[0078] However, if it has repeated storing in a memory card 109 the file which consists of two or more blocks, or deleting it, the fragmentation of a logical block will increase. That is, as shown in drawing 13 (a), in spite of being the logical block which constitutes the same file file1, those logical addresses will become discontinuity.

[0079] Now, since it cannot write to the logical continuation field of a memory card 109 for example, when it is going to store music data in a memory card 109, it will be necessary to publish a write command "Write address count" for every block, and drawing speed will fall. Similarly, in spite of being music data which constitute one music also in read-out actuation, it will be necessary to read for every block and to publish a command "Read address count", and real-time playback of music data will be difficult.

[0080] As an approach of solving this problem, the control IC 302 of this memory card 109 has the function which rewrites a translation table 1101 based on the command from an external instrument. Specifically, the command judging control section 322 of control IC 302 will rewrite a translation table 1101 using the parameter which interprets the command and is sent continuously, if the device dependent command for rewriting a translation table 1101 is inputted from a command pin.

[0081] The concrete actuation is as being shown in drawing 13 . Before the above-mentioned device dependent command is sent now, as a flash memory 303 is shown in drawing 13 (a), the data which constitute a file file1 exist in physical addresses 0 and 2, and suppose that the data which constitute a file file2 in a physical address 1 exist. And as shown in a translation table 1101 at drawing 13 (c), suppose that the contents a physical address and whose logical address correspond are held. That is, suppose that the data of a file file2 are inserted into the data of another file file1, and are stored on the logical address like a physical address top.

[0082] the external instrument which will be obtained and carried out if I will cancel such a condition sends the above-mentioned device dependent command and parameter which show the purport which secures the continuity of the specific file file1 to a flash memory 303. Then, the command judging control section 322 of a memory card 109 rewrites a translation table 1101 by the contents shown in drawing 13 (d) according to the device dependent command and parameter. That is, the logic of a flash memory 303 and the correspondence relation of a physical address are changed as shown in drawing 13 (b).

[0083] As shown in the related Fig. shown in drawing 13 (b), although arrangement of a physical block is not changing, it is rearranged so that two logical blocks which constitute a file file1 may continue. By this, the external instrument is that a twist can also access a file file1 at a high speed till then after next access.

[0084] the authentication field 332 of not only in order that modification of the above translation tables 1101 may fix the fragmentation of a logical block, but the flash memory 303, and the non-attesting field 331 -- it is used also when changing each size. Since what is necessary is just to rewrite a translation table 1101 so that it may be assigned as a physical block of the field where the physical block of the field which makes size small enlarges size at this time, high-speed field modification is attained.

[0085] Next, the function about the non-eliminated block which this memory card 109 has, and the actuation at the time of specifically receiving a non-eliminated list command and an elimination command are explained. Here, a non-eliminated block is a physical block in a flash memory 303, writing was performed in the past and the block

which is in the condition of not eliminating, physically is said. That is, a non-eliminated block is a physical block for which package elimination is needed, before being used for a degree (written in).

[0086] Moreover, the command judging control section 322 is one of the commands in which an interpretation and activation are possible, and a non-eliminated list command is a command for acquiring the list of the numbers of all non-eliminated blocks that exist in the flash memory 303 at the time. Before the flash memory 303 currently used for the memory card 109 writes in, package elimination in a block unit is needed, but since the elimination processing occupies about the one half of write-in time amount, the direction eliminated beforehand can write it in a high speed more. Then, this memory card 109 provides the external instrument with the non-eliminated list command and the elimination command, in order to give those facilities.

[0087] Now, let a flash memory 303 be the busy condition of a logical block as shown in drawing 14 (a), and a physical block. Here, logical blocks 0-2 are using it, and physical blocks 0-2, and 4 and 5 have become a non-eliminated block. In this condition, the non-eliminated list 1203 currently held in the command judging control section 322 serves as contents shown in drawing 14 (b). Here, the non-eliminated list 1203 is a storage table which consists of an entry corresponding to all the physical blocks that constitute a flash memory 303, and the value (in "0" and not eliminating, it is "1" when finishing [elimination]) according to the elimination condition of a corresponding physical block is held under control by the command judging control section 322.

[0088] Drawing 14 (c) is the flow Fig. showing actuation in case PC102 and a player 201 eliminate a block in advance using a non-eliminated list command and an elimination command in such a condition. In addition, as shown in drawing 14 (d), tables, such as FAT (File Allocation Table) which shows the busy condition of a logical block, shall be stored in a flash memory 303.

[0089] PC102 and the external instrument of player 201 grade publish a non-eliminated list command to this memory card 109 in the idle time which access to a memory card 109 has not generated (S1201). The command judging control section 322 of the memory card 109 which received the command is referring to the non-eliminated list 1203 which it has inside, specifies the numbers 0-2 of the physical block into which status value 1 is registered, and 4 and 5, and returns it to the external instrument.

[0090] Then, an external instrument is referring to the table showing the busy condition of the logical block shown in drawing 14 (d) stored in the flash memory 303,

and the block which is not used logically is specified (step S1202). And based on the information acquired at the two above-mentioned steps S1201 and S1202, an eliminable block, i.e., the elimination command which specified the number of these blocks 4 and 5 to (step S1203) and a memory card 109 after specifying a block [**** / un-] (here, they are physical blocks 4 and 5) physically [did not use it logically and], is published (step S1204). The command judging control section 322 of the memory card 109 which received the command carries out package elimination of the physical blocks 4 and 5 specified by taking out directions to the access-control sections 325 and 326 etc.

[0091] Since the elimination processing to the physical block becomes unnecessary by this when the writing to the physical blocks 4 and 5 occurs, high-speed writing is attained. Next, the function about protection of the personal data which this memory card 109 has, and in case a memory card 109 specifically attests an external instrument, the protection feature of the personal data in the case of needing the personal data of the user who uses that external instrument is explained. Here, personal data are data for identifying the user uniquely, and are data for making a memory card 109 identify as a user of normal to whom access to the authentication field 332 of a memory card 109 was permitted.

[0092] In such a case, it sets and there is un-arranging [which requires the thing to the authentication field 332 for which personal data are repeatedly inputted at every access to a user, is intercepted by the inaccurate person in our having decided to store the personal data in the authentication field 332, or is looked at by other users who have the authority to access the authentication field 332].

[0093] In order to prevent this, how to store after enciphering about personal data as well as music data with the password which the individual set up can be considered. However, when a password is set up, whenever it sees the personal data, a password must be entered, a procedure is troublesome and the management is also needed. Then, this memory card 109 has the function to avoid repeating and inputting personal data superfluously.

[0094] Drawing 15 is drawing showing the communication link sequence and the main components between the player 201 for authentication, and a memory card 109. In addition, processing shown in this Fig. is mainly realized by the authentication circuit 216 of a player 201, and the authentication section 321 of a memory card 109. As shown in this Fig., the authentication circuit 216 of a player 201 has remembered beforehand device-dependent [which is ID of a proper / ID / 1302] to be the master key 1301 which is the same private key as master key 323a held at the memory card

109 other than functions, such as encryption and a decryption, to the players 201, such as a serial number (second/n).

[0095] Moreover, otherwise, the authentication section 321 of a memory card 109 has the device-dependent ID group storage region 1310 and the user key storage region 1311 which are two storage regions [**** / un-] in functions, such as encryption, a decryption, and a comparison. The device-dependent ID group storage region 1310 is a storage region for memorizing device-dependent [of all the devices by which access to the authentication field 332 of this memory card 109 was permitted / ID], and the user key storage region 1311 is a storage region for memorizing the user key sent from the device as personal data.

[0096] The concrete authentication procedure is as follows. In addition, in transmission and reception, it is enciphered and transmitted and all data are decoded by the receiving side. And the key used for encryption and a decryption with the following procedure whenever a procedure progresses is generated.

(1) If a memory card 109 and a player 201 are connected, first, a player 201 will encipher device-dependent [ID / 1302] using the master key 1301, and will send it to a memory card 109.

[0097] (2) A memory card 109 inspects whether device-dependent [which was received / which was enciphered / ID / 1302] is decoded by master key 323a, and device-dependent [which was obtained / ID / 1302] is already stored in the device-dependent ID group storage region 1310.

(3) Consequently, notify the purport that authentication was successful when device-dependent [ID / 1302] was already stored to a player 201, and on the other hand, when device-dependent [ID / 1302] is not stored, require a user key from a player 201.

[0098] (4) After a player 201 demands the input of a user key from a user, it acquires the user key as personal data from a user, and sends the user key to a memory card 109.

(5) It stores in the device-dependent ID group storage region 1310 device-dependent [which was gained at the above-mentioned step (3) / ID / 1302] while a memory card 109 compares the sent user key with the thing beforehand stored in the user key storage region 1311, and it notifies the purport that authentication was successful to a player 201, when in agreement, or when the user key storage region 1311 is empty.

[0099] When the device and memory card 109 which a user owns are connected for the first time by this, the input of personal data (user key) is needed, but since device-dependent [of the device / ID] is used for 2nd henceforth and authentication

is automatically successful, the input of personal data is not required again. Next, the modification of the Challenge Handshake Authentication Protocol of this memory card 109, and a PC102 and the external instrument of player 201 grade is explained using drawing 16 and drawing 17 .

[0100] Drawing 16 is the communication link sequence diagram showing the authentication procedure of the memory card 109 and external instrument (here player 201) concerning a modification. Processing here is mainly realized by the authentication section 321 of the control program 111b and the memory card 109 of the authentication circuit 216 of the player 201 concerning a modification, and PC102. moreover, the enciphered master key (encryption master key 323b) stores in the master key storage section 323 of a memory card 109 -- having -- **** -- the special field 304 -- media ID 341 -- in addition, the secure media ID 343 which encipher the media ID 341 and are obtained shall be stored

[0101] First, a player 201 is emitting a command to a memory card 109, takes out master key 323b of a memory card 109, and decodes it by device key 211a. A decode algorithm here corresponds to the cryptographic algorithm used when encryption master key 323b stored in the memory card 109 was generated. Therefore, if device key 211a which this player 201 has was planned (thing of normal), this decode will revert to the original master key.

[0102] Then, a player 201 is emitting a command to a memory card 109, takes out the media ID 341 of a memory card 109, and enciphers them with the restored above-mentioned master key. Cryptographic algorithm here is the same as that of the cryptographic algorithm used when the secure media ID 343 stored in the memory card 109 were generated. Therefore, the same secure media ID as the secure media ID 343 which a memory card 109 has are obtained by encryption here.

[0103] Then, a player 201 and a memory card 109 perform mutual recognition using each of these secure media ID. Consequently, also in which device, the information which shows whether it succeeded in authentication of a phase hand-loom machine (OK/NG), and the secure key which is a strange key when becoming settled depending on the authentication result are generated. This secure key has the property changed whenever it repeats mutual recognition only in accordance with the case where both devices 201 and 109 succeed in authentication.

[0104] Then, if it succeeds in mutual recognition, a player 201 will generate the command for accessing the authentication field 332 of a memory card 109. If it is the case where data are read from the authentication field 332, the parameter (the address "address" of 24 bit length and count of 8 bit length "count") of the command

"SecureReadaddress count" will be enciphered with a secure key, and, specifically, the encryption command which connects the obtained encryption parameter and the tag (code of 6 bit length which shows the class "SecureRead" of command) of the command, and is obtained will be sent to a memory card 109.

[0105] The memory card 109 which received the encryption command judges the class of command from the tag. Here, it judges with it being a read-out command "SecureRead" from the authentication field 332. Consequently, when it judges with it being an access command to the authentication field 332, the parameter contained in the command is decoded with the secure key obtained by mutual recognition. Since a decode algorithm here corresponds to the cryptographic algorithm used when generating an encryption command in a player 201, if mutual recognition was successful (i.e., if the secure key used by both devices is in agreement), the parameter obtained by this decode will become equal to the original parameter used by the player 201.

[0106] And a memory card 109 reads the cryptographic key 425 stored in the sector specified with the decoded parameter from the authentication field 332, enciphers it with a secure key, and transmits to a player 201. A player 201 decodes the sent data using the secure key obtained by mutual recognition. Since a decode algorithm here is equivalent to the algorithm used for encryption of a cryptographic key 425 in the memory card 109, if mutual recognition was successful (i.e., if the secure key used by both devices is in agreement), the data obtained by this decode are in agreement with the original cryptographic key 425.

[0107] In addition, a memory card 109 cancels the secure key used for it whenever it finished activation of the access command to the authentication field 332 (elimination). By this, whenever the external instrument which accesses the authentication field 332 of a memory card 109 sent out one command, it needed to perform mutual recognition in advance, and it needs to pass it to it. Drawing 17 is the communication link sequence diagram showing the detailed procedure in the mutual recognition shown in drawing 16 . Here, a memory card 109 and a player 201 perform mutual recognition of a challenge response mold.

[0108] In order to verify the justification of a player 201, a memory card 109 generates a random number and sends it to a player 201 by making it into challenge data. In order to prove self justification, a player 201 enciphers the challenge data and returns it to a memory card 109 as response data. A memory card 109 compares the response data with the encryption challenge data which encipher the random number sent as challenge data, and are obtained, when in agreement, recognizes it as (O.K.) which

succeeded in authentication of a player 201, and receives the access command to the authentication field 332 sent from the player 201. On the other hand, the activation is refused, even if it has recognized it as having carried out (NG) which did not succeed in authentication and the access command from the player 201 to the authentication field 332 has been sent after that, when not in agreement as a result of a comparison.

[0109] Similarly, a player 201 performs the same exchange as the above-mentioned authentication, in order to verify the justification of a memory card 109. That is, a random number is generated and it sends to a memory card 109 by making it into challenge data. In order to prove self justification, a memory card 109 enciphers the challenge data, and returns it to a player 201 as response data. A player 201 compares the response data with the encryption challenge data which encipher the random number sent as challenge data, and are obtained, when in agreement, recognizes it as (O.K.) which succeeded in authentication of a memory card 109, and performs AKUSESUKO to the authentication field 332 of the memory card 109. On the other hand, when not in agreement as a result of a comparison, it is recognized as having carried out (NG) which did not succeed in authentication, and access to the authentication field 332 of the memory card 109 is given up.

[0110] In addition, the encryption algorithm in these mutual recognition is altogether the same as long as a memory card 109 and a player 201 are just devices. Moreover, a memory card 109 and a player 201 carry out EXCLUSIVE OR operation of the encryption challenge data and response data which were generated in each authentication and certification, and they are used for them by using the obtained result as a secure key for access to the authentication field 332 of a memory card 109. doing so -- things -- both sides -- a device -- 109 -- and -- 201 -- mutual recognition -- having succeeded -- a case -- being common -- ** -- becoming -- and -- the time -- being strange -- secure ones -- a key -- sharing -- suiting -- things -- being possible -- ** -- becoming -- this -- authentication -- a field -- 332 -- accessing -- conditions -- ****** -- mutual recognition -- succeeding -- **** -- things -- conditions -- ** -- carrying out -- having -- ******** .

[0111] In addition, it is good as a generation method of a secure key also as taking the exclusive OR of encryption challenge data, response data, and the secure media ID. Next, the modification about the modification function of the boundary line of the authentication field 332 of this memory card 109 and the non-attesting field 331 is explained using drawing 18 and drawing 19 . Drawing 18 is drawing showing the busy condition of the flash memory 303 before changing a boundary line. Drawing 18 (a) is a memory map in which the configuration of the physical block of a flash memory 303 is

shown.

[0112] Drawing 18 (b) is the translation table 1103 of non-attesting field 331 dedication put on a storage region [**** / in the non-attesting field access-control section 326 / un-] etc., and the correspondence relation between the logical block of the non-attesting field 331 and a physical block is stored. By referring to this translation table 1103, the non-attesting field access-control section 326 can change the logical address into a physical address, or can detect violation of access exceeding a quota field.

[0113] Drawing 18 (c) is the translation table 1102 of authentication field 332 dedication put on a storage region [**** / in the authentication field access-control section 325 / un-] etc., and the correspondence relation between the logical block of the authentication field 332 and a physical block is stored. By referring to this translation table 1102, the authentication field access-control section 325 can change the logical address into a physical address, or can detect violation of access exceeding a quota field.

[0114] As shown in drawing 18 (a) before modification of a boundary line, the physical block 0000 located in a lower address rather than a boundary line among the storage regions (a physical block 0000 - EFFF) except the alternative field of a flash memory 303 - DFFF are assigned to the non-attesting field 331, and the physical block E000 located in an upper address - EFFF are assigned to the authentication field 332.

[0115] And in the non-attesting field 331, as shown in the translation table 1102 shown in drawing 18 (b), it is matched so that the number of a physical block and a logical block may be in agreement. As shown on the other hand in the translation table 1103 shown in drawing 18 (c), in the authentication field 332, as for the physical block and the logical block, the list of the number is a reverse order. That is, a logical block 0000 - each 0FFF support physical block EFFF-E000. This is because the logical block took into consideration the time and effort of being used for ascending order, data evacuation of the physical block which field modification produced when a boundary line was moved, or migration processing.

[0116] Drawing 19 (a) - (c) is drawing showing the busy condition of the flash memory 303 of Ushiro who changed the boundary line, and corresponds to drawing 18 [before modification] (a) - (c), respectively. In addition, modification of a boundary line is realized when the command of the dedication which specifies the address is inputted into the command judging control section 322 from a command pin, and the translation table 1102 in the authentication field access-control section 325 and the translation table 1103 in the non-attesting field 331 are rewritten by the command judging control

section 322.

[0117] Drawing 19 (a) As shown in - (c), the boundary line placed between a physical block E000 and DFFF is moved between a physical block D000 and CFFF here. That is, only 1000 (hex) individual decreases the size of the non-attesting field 331, and only 1000 (hex) is making the size of the authentication field 332 increase. In connection with it, as shown in drawing 19 (b), the size of the translation table 1103 of the non-attesting field 331 decreases an entered part of 1000 (hex) individuals, consequently the physical block 0000 corresponding to a logical block 0000 - CFFF - CFFF are shown. On the other hand, as shown in drawing 19 (c), it is increased by the size of the translation table 1102 of the authentication field 332 an entered part of 1000 (hex) individuals, consequently physical block EFFF-D000 corresponding to logical-block 0000-1FFF is shown.

[0118] Thus, it becomes possible by changing a non-attesting field and an authentication field according to a boundary line, and changing the size of each field by migration of a break and its boundary line in the fixed field of a flash memory 303, to make it correspond, when making into main applications various application of this memory card 109, for example, storing of the digital work which should be protected, or when [that] reverse.

[0119] and a non-attesting field and an authentication field -- also in any, time and effort accompanying migration of a boundary line, such as data evacuation and migration processing, is reduced by matching a logical block and a physical block so that it may be used toward the physical block of the address near a boundary line from the physical block of the address distant from a boundary line. Moreover, such matching is separating into the translation table 1102 of authentication field 332 dedication, and the translation table 1103 of non-attesting field 331 dedication, and preparing, and it becomes easy the to realize it.

[0120] In addition, in the authentication field 332, although the logical address and a physical address had become a reverse order in the unit of a block, it is not restricted to such a unit, for example, is good in a cutting tool's unit also as a reverse order in considering as a reverse order in the unit of a sector. As mentioned above, although the memory card of this invention was explained using the gestalt and modification of operation, this invention is not limited to these.

[0121] For example, although authentication with the memory card 109 by the procedure same whenever it emits the command for accessing the authentication field 332 of a memory card 109 was needed, you may enable it to access PC102 and a player 201 in the authentication procedure simplified depending on the class of

command. For example, about a write command "SecureWrite", though it is necessary to take out neither encryption master key 323b nor media ID 341 from a memory card 109, it only succeeds in authentication of a uni directional (authentication of the device by the memory card 109) and a memory card 109 performs, it is good. The execution speed is accelerated by this about the command whose relation with protection of copyrights is not so strong.

[0122] Moreover, even if it transposes the flash memory 303 which the memory card 109 of this invention has to non-volatilized media, such as other storage media, for example, a hard disk, an optical disk, and a magneto-optic disk, it cannot be overemphasized that the pocket mold storage card in which the same protection of copyrights as this invention is possible is realized.

[0123]

[Effect of the Invention] The semi-conductor memory card concerning this invention so that clearly from the above explanation It is a semi-conductor memory card removable on electronic equipment. Rewritable nonvolatile memory, It has the control circuit which controls access by said electronic equipment to the authentication field and the non-attesting field which are two storage regions where it was beforehand set in said nonvolatile memory. Said control circuit The non-attesting field access-control section which controls access by said electronic equipment to said non-attesting field, It is characterized by having the authentication section which tries authentication of said electronic equipment in order to verify the justification of said electronic equipment, and the authentication field access-control section which permits access by said electronic equipment to said authentication field only when said authentication section succeeds in authentication.

[0124] It can be used by storing the data in connection with protection of copyrights in an authentication field, and storing in a non-attesting field by this, the data which are not so, making a digital work and a non-work intermingled, and the semi-conductor memory card which has both applications is realized. Said authentication section generates the key data reflecting the result of authentication here, and though said authentication field access-control section is decoded by the key data by which said authentication section generated the enciphered instruction which is sent from said electronic equipment and controls access to said authentication field according to the decoded instruction, it is good.

[0125] Even if the exchange with a semi-conductor memory card and electronic equipment is intercepted by this, since it is enciphered by it depending on the authentication result to which the instruction for accessing an authentication field

was carried out immediately before, by it, the prevention function to unjust access to an authentication field becomes high. Moreover, though said authentication section generates said key data from the response data generated in order to prove the challenge data transmitted to said electronic equipment in order to perform mutual recognition of said electronic equipment and a challenge response mold and to verify the justification of said electronic equipment, and self justification, it is good.

[0126] The safety of the authentication field which cannot be accessed by this if such key data are not used for them, since key data have the property to be shared in both sides for the first time only when the both sides of a semi-conductor memory card and electronic equipment succeed in mutual recognition, and to change at every authentication becomes a stronger thing. Moreover, the enciphered instruction which is sent from said electronic equipment It consists of the tag section which specifies the classification of access to said authentication field and which is not enciphered, and enciphered address part which pinpoints the field to access. Said authentication section It is good though execution control of the access of the classification specified by the tag section of said instruction is carried out to the field which decodes the address part of said instruction and is pinpointed by the decoded address using said key data.

[0127] Since only the address part of an instruction is enciphered by this, by it, the decode by the semi-conductor memory card and decode processing in which such an instruction was received become simple. Moreover, said semi-conductor memory card is equipped with the discernment data store circuit which memorizes beforehand the discernment data of the proper which can specify self in distinction from the semi-conductor memory card of further others, and though said authentication section performs mutual recognition using the discernment data stored in said discernment data store circuit, makes it dependent on said discernment data and generates said key data, it is good.

[0128] In mutual recognition, since it is exchanged in the data depending on each semi-conductor memory card by this, high safety is maintainable to decode of inaccurate mutual recognition with this. Moreover, said semi-conductor memory card may be further equipped with the area-size modification circuit which changes the area size of said authentication field and each of said non-attesting field. By this, at a certain time, a semi-conductor memory card is mainly used as a record medium of a digital work, or dynamic modification for various applications, such as using as an auxiliary storage unit of a computer system, is attained at a certain time.

[0129] Moreover, said authentication field and said non-attesting field are assigned to

each field obtained by carrying out the storage region where the fixed size in said nonvolatile memory continued for 2 minutes, and though said area-size modification circuit changes the area size of said authentication field and each of said non-attesting field by changing the boundary address which carries out the storage region of said fixed size for 2 minutes, it is good. By this, since the area size of an authentication field and a non-attesting field can be changed only by moving a boundary line, the circuit for it is small and ends.

[0130] Moreover, the authentication field translation table showing correspondence with the logical address and a physical address, [in / in said area-size modification circuit / said authentication field] The non-attesting field translation table showing correspondence with the logical address and the physical address in said non-attesting field, It has the translation table modification section which changes said authentication field translation table and said authentication field translation table according to the instruction from said electronic equipment. Said authentication field access-control section Access by said electronic equipment is controlled based on said authentication field translation table, and though said non-attesting field access-control section controls access by said electronic equipment based on said non-attesting field translation table, it is good.

[0131] By this, in an authentication field and a non-attesting field, since the translation table has gained separate independence, it becomes easy to manage correspondence with each area size, logical address, and physical address according to an individual. Moreover, said authentication field and said non-attesting field are assigned to the high field and the low field of the physical address obtained by carrying out the storage region of said fixed size for 2 minutes, respectively, the logical address and a physical address are matched so that the ascending order of the logical address may turn into ascending order of a physical address, and said authentication field translation table is good [as for said non-attesting field translation table], though the logical address and a physical address are matched so that the ascending order of the logical address may turn into descending order of a physical address.

[0132] By using it for the ascending order of the logical address, since the establishment for which the field near the boundary of an authentication field and a non-attesting field is used becomes low, the probability for processing of data evacuation, migration, etc. which are needed when the boundary is moved to occur also becomes low, and modification of area size is simplified by this. Moreover, said semi-conductor memory card may be equipped with the read-only memory circuit in which data were stored further beforehand. The function of protection of copyrights is

strengthened with storing discernment data distinguishable from other semi-conductor memory cards etc. in a read-only memory, making it dependent on the discernment data, and storing a digital work by this.

[0133] Moreover, said authentication field and said non-attesting field consist of a storage region which can be written for said electronic equipment, and a read-only storage region. Said control circuit has the random number generator which generates a random number whenever it accesses further for said electronic equipment writing data in said nonvolatile memory. Said authentication field access-control section and said non-attesting field access-control section While enciphering and writing said data in the storage region which can write [said] the obtained encryption data using said random number, it is good though said random number is written in said read-only storage region matched with said encryption data.

[0134] Since it becomes possible to detect such an action by inspecting adjustment with the random number stored in the read-only storage region even if the unjust alteration to the storage region which can be written etc. is performed by this, safer data logging is realized. Moreover, said control circuit has further the translation table showing correspondence with the logical address and the physical address in said authentication field and said non-attesting field, and the translation table modification section which changes said translation table according to the instruction from said electronic equipment, and though said authentication field access-control section and said non-attesting field access-control section control access by said electronic equipment based on said translation table, they are good.

[0135] Since it can change easily so that it may become the logical block which continued logically even if the phenomenon which two or more logical blocks which constitute the same file fragment by this arises, access to the same file is accelerated. Moreover, said control circuit may have the code decode section which decrypts the data read from said authentication field and said non-attesting field while enciphering further the data which should be written in said authentication field and said non-attesting field. A semi-conductor memory card is destroyed and this enables it to be equal to the unjust attack of reading the memory content of an authentication field and a non-attesting field directly.

[0136] Moreover, said nonvolatile memory is a flash memory, and said control circuit may pinpoint further the field which is not eliminated [which exists in said authentication field and said authentication field] according to the instruction from said electronic equipment, and may have the non-eliminated list read-out section which sends the information which shows the field to said electronic equipment. By

this, since electronic equipment can know a non-eliminated field and can eliminate the field in advance in advance of rewriting of a flash memory, high-speed rewriting of it is attained.

[0137] Moreover, the user key storage section for said authentication section to require the user key which is the information on a proper of the user from the user who uses electronic equipment for authentication, and for said control circuit memorize said user key further, The identification information storage section for memorizing the identification information which can specify the electronic equipment which succeeded in authentication by said authentication section, If authentication by said authentication section is started, identification information will be acquired from the electronic equipment. When the identification information inspects whether it is already stored in said identification information storage section and is already stored in it, you may have the user key demand prohibition section in which the demand of the user key by said authentication section is forbidden.

[0138] Since the time and effort that the input of a password or personal data is required whenever it uses it for a semi-conductor memory card by this, connecting is avoided, generating of the fault that personal data are intercepted and used unjustly is suppressed. The read-out equipment concerning this invention is read-out equipment which reads the digital work stored in the above-mentioned semi-conductor memory card. Said semi-conductor memory card While the digital work is stored in the non-attesting field, the count which permits read-out of said digital work is beforehand stored in an authentication field. Said read-out equipment A decision means to judge whether the count stored in said authentication field is read, and read-out is permitted by the count in case the digital work stored in said non-attesting field is read, Only when the permission is granted, while reading said digital work from said non-attesting field, it is characterized by having the playback means which subtracts said read count and is returned to said authentication field.

[0139] By this, it becomes possible to restrict the count of read-out of the digital work stored in the semi-conductor memory card, and becomes applicable to the charged rental of a music content etc. Moreover, the read-out equipment concerning this invention is read-out equipment which reads the digital work stored in the above-mentioned semi-conductor memory card, and is reproduced to an analog signal. While the digital work refreshable to an analog signal is stored in the non-attesting field, said semi-conductor memory card The count which permits the digital output by said electronic equipment of said digital work is beforehand stored in an authentication field. Said read-out equipment A playback means to read the digital

work stored in said non-attesting field, and to reproduce to an analog signal, Only when the permission is granted with a decision means to judge whether the count stored in said authentication field is read, and the digital output is permitted by the count, while outputting said digital work outside with a digital signal It is characterized by having the digital output means which subtracts said read count and is returned to said authentication field.

[0140] It becomes possible to restrict the count of the digital copy of the digital work stored in the semi-conductor memory card by this, and the fine protection of copyrights of the grain in alignment with an intention of a copyright person becomes possible. Thus, this invention is a semi-conductor memory card which has the flexible function which combines both the application as a record medium of a digital work, and the application as an auxiliary storage unit of a computer, the effectiveness of securing healthy circulation of the digital work accompanying an electronic music distribution especially is done so, and the practical value is very large.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] They are a personal computer concerning the electronic music distribution in the gestalt of operation of this invention, and drawing showing the appearance of a removable semi-conductor memory card in the PC.

[Drawing 2] It is drawing showing the appearance of the player of the pocket mold which uses this semi-conductor memory card as a record medium.

[Drawing 3] It is the block diagram showing the hardware configuration of this personal computer.

[Drawing 4] It is the block diagram showing the hardware configuration of this player.

[Drawing 5] It is drawing showing the appearance and hardware configuration of this semi-conductor memory card.

[Drawing 6] It is drawing showing the class of storage region of this semi-conductor memory card seen from this personal computer or this player.

[Drawing 7] (a) shows the Ruhr in access to each field, it is drawing showing the limit at the time of this personal computer and this player accessing each field of this semi-conductor memory card, and the gestalt of a command, and (c) is [(b) shows the Ruhr in modification of the size of each field, and] the conceptual diagram showing the field of this semi-conductor memory card.

[Drawing 8] It is the flow Fig. showing the actuation in which this personal computer (and this player) writes contents, such as music data, in this semi-conductor memory card.

[Drawing 9] It is the flow Fig. showing the actuation which reads contents, such as music data, from this semi-conductor memory card, and is reproduced by this player (and this personal computer).

[Drawing 10] This player (and this personal computer) is the flow Fig. showing the actuation which was stored in the authentication field of this semi-conductor memory card, and which reads and operates a count.

[Drawing 11] This player (and this personal computer) is the flow Fig. showing the actuation which operates the count of digital output authorization stored in the authentication field of this semi-conductor memory card.

[Drawing 12] It is drawing showing DS common to the authentication field and the non-attesting field of this semi-conductor memory card, and the flow of the R/W processing corresponding to the DS.

[Drawing 13] It is drawing showing signs that correspondence with the logical address of this semi-conductor memory card and a physical address is changed, and the translation table corresponding to [(a)] (a) in (c) and (d) show the translation table corresponding to (b) corresponding to the correspondence relation after modification in the correspondence relation before modification, and (b).

[Drawing 14] (b) shows the non-eliminated list in the condition, it is drawing explaining the function about the non-eliminated block which this semi-conductor memory card has, and (d) is [(a) shows the busy condition of a logical block and a physical block and / (c) is the flow Fig. showing actuation in case PC102 and a player 201 eliminate a

block in advance using a non-eliminated list command and an elimination command, and] the table showing the busy condition of a logical block.

[Drawing 15] It is drawing showing the communication link sequence and the main components between this player for authentication, and this semi-conductor memory card.

[Drawing 16] It is the communication link sequence diagram showing the authentication procedure of the this semi-conductor memory card and external instrument concerning the modification of this invention.

[Drawing 17] It is the communication link sequence diagram showing the detailed procedure of mutual recognition shown in drawing 16 .

[Drawing 18] It is drawing showing the condition before modification in modification of the boundary line of the authentication field of this semi-conductor memory card, and a non-attesting field, and (a) is a memory map in which the configuration of the physical block of a flash memory is shown, (b) shows the translation table only for non-attesting fields, and (c) shows the translation table only for authentication fields.

[Drawing 19] It is drawing showing the condition after modification in modification of the boundary line of the authentication field of this semi-conductor memory card, and a non-attesting field, and (a) is a memory map in which the configuration of the physical block of a flash memory is shown, (b) shows the translation table only for non-attesting fields, and (c) shows the translation table only for authentication fields.

[Description of Notations]

101 Communication Line
102 PC
103 Display
104 Keyboard
105 Memory Card Writer Insertion Opening
106 Loudspeaker
107 Memory Card Writer
108 Memory Card Insertion Opening
109 Memory Card
110 CPU
111 ROM
112 RAM
113 Communication Link Port
114 Internal Bus
117 Descrambler

118 AAC Decoder
119 D/A Converter
120 Hard Disk
201 Player
202 Manual Operation Button
203 Liquid Crystal Display Section
204 Analog Output Terminal
205 Digital Output Terminal
206 Memory Card Insertion Opening
208 Headphone
210 CPU
211 ROM
212 RAM
213 Communication Link Port
214 Internal Bus
215 Card I/F Section
216 Authentication Circuit
217 Descrambler
218 AAC Decoder
219 D/A Converter
220 AAC Encoder
221 A/D Converter
222 Scrambler
223 Analog Input Terminal
224 Loudspeaker
302 Control IC
303 Flash Memory
304 ROM (Special Field)
321 Authentication Section
322 Command Judging Control Section
323 Master Key Storage Section
323a Master key
323b Encryption master key
324 Special Field Access-Control Section
325 Authentication Field Access-Control Section
326 Non-Attesting Field Access-Control Section

327 Code and Decryption Circuit
331 Non-Attesting Field
332 Authentication Field
341 Media ID
342 Manufacture Manufacture Name
343 Secure Media ID
425 Cryptographic Key
426 Encryption Contents
427 User Data
501 Alternative Block Field
812 Count of Read-out
913 Count of Digital Output Authorization
1003 Random Number Generator
1004 Sector
1005 Extended Partition
1006 ECC Data
1007 the Time -- Strange Field
1101 Translation Table
1102 Translation Table Only for Authentication Fields
1103 Translation Table Only for Non-Attesting Fields
1203 Non-Eliminated List
1301 Master Key
1302 Device-dependent [ID]
1310 Device-dependent ID Group Storage Region
1311 User Key Storage Region